

# A Comprehensive Analysis of Security Mechanisms and Threat Characterization in Mobile Ad Hoc Networks

<sup>1</sup>Vikas, <sup>2</sup>Dr. Shashiraj Teotia

Department of Computer Application, Swami Vivekanand Subharti University, Meerut U.P India

DOI: <https://doi.org/10.51583/IJLTEMAS.2025.140500079>

Received: 31 May 2025; Accepted: 09 June 2025; Published: 19 June 2025

**Abstract:** Mobile Ad Hoc Networks (MANETs) represent a critical advancement in wireless communication, enabling dynamic, infrastructure-less networking suitable for various applications, including military, disaster recovery, and remote sensing. However, their decentralized architecture, dynamic topology, and constrained resources expose them to a wide range of security challenges. This research paper presents a comprehensive evaluation of existing security mechanisms designed to protect MANETs, encompassing cryptographic protocols, intrusion detection systems, secure routing techniques, and trust-based frameworks. By systematically analyzing their effectiveness, limitations, and adaptability, the study highlights gaps in current approaches. Additionally, this work identifies and characterizes MANET-specific security threats, including wormhole, black hole, sybil, and denial-of-service attacks. Through this dual-focused investigation, the paper not only maps the current landscape of MANET security solutions but also provides a structured threat taxonomy, offering insights into the evolving threat model. The findings aim to guide the development of more robust, adaptive, and context-aware security frameworks tailored for MANET environments.

**Keywords**—Intrusion detection, Secure routing, Decentralized networks, Network vulnerabilities, Attack taxonomy.

## INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have gained considerable attention in recent years as a critical paradigm in wireless networking. Unlike traditional networks that rely on a centralized infrastructure such as routers, switches, or access points, MANETs are composed of a collection of mobile nodes that dynamically form a temporary network without any fixed infrastructure or centralized administration. This inherent flexibility and adaptability make MANETs particularly well-suited for various applications, including military communications, disaster recovery operations, vehicular networks, mobile health services, and remote environmental monitoring. In such environments, the ability to quickly establish communication links among nodes without relying on fixed infrastructure becomes crucial. Despite their potential, MANETs face significant challenges, among which security stands out as one of the most critical and complex issues. The decentralized and open nature of MANETs exposes them to a wide range of security vulnerabilities and threats. In contrast to traditional wired or infrastructure-based wireless networks, MANETs are inherently more vulnerable due to their unique characteristics. These include dynamic network topology, lack of centralized control, node mobility, limited bandwidth, constrained energy resources, and the open wireless communication medium. Together, these factors make it difficult to implement conventional security measures and ensure reliable and secure communication among nodes. The dynamic nature of node movement within MANETs results in frequent topology changes, which complicates routing and increases the risk of routing-based attacks. The lack of centralized authority means there is no single point of control to manage trust, authentication, or access control. Moreover, since nodes in a MANET often rely on battery power and have limited processing capabilities, implementing resource-intensive cryptographic or intrusion detection algorithms can severely degrade network performance. This makes the trade-off between security and resource efficiency a major consideration in the design of MANET security mechanisms. Over the years, researchers have proposed various security solutions to address these challenges. These solutions include encryption techniques for data confidentiality, secure routing protocols to defend against routing attacks, intrusion detection systems (IDS) to monitor and respond to suspicious activities, and trust management models to establish node reliability. Examples include protocols like Secure AODV (Ad hoc On-demand Distance Vector), ARAN (Authenticated Routing for Ad hoc Networks), and SAODV, each tailored to mitigate specific types of attacks. While these solutions offer a degree of protection, none are universally effective. The effectiveness of a particular security mechanism often depends on the specific context in which it is deployed, such as network size, mobility patterns, attack types, and the presence of malicious or compromised nodes. Furthermore, many existing approaches either fail to scale well or impose significant overhead on the already constrained resources of mobile devices.

In parallel with the development of security mechanisms, the threat landscape for MANETs has evolved and diversified. Several types of attacks are unique or particularly potent in MANET environments. For example, a black hole attack involves a malicious node falsely advertising a shortest path to a destination, thereby attracting and dropping all packets, disrupting data transmission. Similarly, in a wormhole attack, two malicious nodes create a tunnel to pass packets secretly between distant parts of the network, undermining routing protocols. Other attacks include sybil attacks, where a single node assumes multiple identities, and denial-of-service (DoS) attacks, which aim to exhaust network resources and make services unavailable. These threats exploit the very characteristics that define MANETs, making their detection and prevention a complex task.

The first objective of this research is to evaluate existing security mechanisms in MANETs. This involves a systematic analysis of current approaches in terms of their design principles, strengths, limitations, and applicability to various real-world scenarios. The evaluation will consider factors such as computational overhead, scalability, detection accuracy, and energy efficiency. Understanding how these mechanisms perform under different conditions will help identify critical gaps and inform the development of more adaptive and efficient security solutions. The second objective is to identify and characterize MANET-specific security threats. Unlike traditional networks, MANETs exhibit vulnerabilities that are deeply intertwined with their architecture and operation. This objective involves the classification of threats based on their impact on network performance, the layer of the network they target (e.g., physical, data link, network, or application), and their method of execution. The goal is to develop a comprehensive threat taxonomy that can serve as a foundation for designing targeted and context-aware defense strategies. Characterizing threats also aids in benchmarking the resilience of proposed security mechanisms against evolving attack vectors. Together, these objectives aim to provide a holistic view of the MANET security landscape. By bridging the gap between existing security mechanisms and the specific threats they aim to mitigate, this research seeks to contribute valuable insights that can guide the future development of more robust and intelligent security architectures for MANETs. The findings will not only advance theoretical understanding but also have practical implications for the deployment of secure MANETs in mission-critical and resource-constrained environments.

## **LITERATURE REVIEW**

The detection and classification of encrypted and malicious network traffic have been widely explored using deep learning techniques. Reddy et al. [1] proposed a deep learning method to detect encrypted and malicious network traffic, achieving improved accuracy. Sharma et al. [2] explored brain-computer interfaces (BCIs) that bridge human brain signals with computing systems, highlighting their potential in healthcare and assistive technologies. Sultana et al. [3] developed a smart traffic management system leveraging IoT and AI to improve mobility and emergency response in urban environments. Kavitha et al. [4] further enhanced this by designing an IoT-based traffic control system dedicated to emergency vehicles. Han et al. [5] introduced a lightweight, unsupervised anomaly detection method for encrypted malware traffic, which is particularly effective in dynamic threat environments. Zhao et al. [6] proposed an error-resilient recurrent neural network (ERNN) model tailored for encrypted traffic detection to handle network-induced variabilities effectively. Zeng et al. [7] presented Deep-Full-Range, a deep learning framework for encrypted traffic classification and intrusion detection. Similarly, Yu et al. [8] designed a neural network-based system to detect encrypted malicious traffic, demonstrating high detection rates. Wang et al. [9] applied one-dimensional convolutional neural networks for end-to-end encrypted traffic classification, underscoring the versatility of CNNs in cybersecurity applications. Yang and Shami [10] explored transfer learning and optimized CNN models for intrusion detection within the Internet of Vehicles, addressing specific security challenges in vehicular networks. Sharma and Kumar [11] emphasized the role of artificial intelligence in enhancing security and privacy of data in smart cities, where IoT devices generate large volumes of sensitive data. Somnath et al. [12] proposed a brain-computer interaction framework based on deep learning to aid patients with speech and motor impairments. Blockchain technology has emerged as a promising solution to IoT security challenges. Kant et al. [13] demonstrated the use of blockchain as a deployment mechanism to secure IoT-based systems, ensuring data integrity and decentralized trust. Vikas et al. [14] combined hybrid deep belief networks with the Harris Hawks optimizer for intrusion detection in wireless sensor networks, illustrating the effectiveness of hybrid AI models in securing IoT environments. Collectively, these studies underline the growing integration of AI, blockchain, and hybrid learning models to tackle emerging security and privacy challenges across network traffic analysis, smart city infrastructure, IoT ecosystems, vehicular networks, and healthcare interfaces.

## **PROPOSED METHODOLOGY**

This research adopts a mixed-methods approach—systematic literature survey, simulation-based experimental evaluation, and security threat modeling—to meet the dual objectives of evaluating existing security mechanisms and identifying MANET-specific threats. The methodology is structured into two phases:

### **Phase I: Evaluation of Existing Security Mechanisms in MANETs**

**Literature Review and Taxonomy Development:** A systematic literature review was conducted using IEEE Xplore, ScienceDirect, SpringerLink, and ACM Digital Library databases. Over 100 research papers published between 2003 and 2025 were reviewed to extract a comprehensive list of existing MANET security mechanisms. Security mechanisms in Mobile Ad Hoc Networks (MANETs) can be classified based on their operational layer and the specific security objectives they address. At the network layer, protocols like SAODV, ARAN, and SEAD secure routing processes against attacks such as blackhole and wormhole by using cryptographic techniques. The transport layer employs protocols such as SSL/TLS and SRTP to ensure secure end-to-end communication through encryption and authentication. At the application layer, lightweight encryption mechanisms safeguard data confidentiality with minimal resource usage. Cross-layer solutions, like CONFIDANT and Watchdog, utilize collaborative monitoring and trust-based systems to detect misbehavior by leveraging information from multiple layers. Additionally, these mechanisms are categorized by their security objectives: authentication (e.g., ARAN, SEAD) verifies node identities; integrity (e.g., SAODV, SEAD) ensures data remains unaltered; confidentiality (e.g., ECC, AES, RSA) protects data from unauthorized access; availability (e.g., Watchdog, OCEAN) ensures network services remain accessible; and trust management (e.g., CONFIDANT, SORI) promotes reliable node behavior through reputation-based models.

**Selection of Benchmark Protocols:** For the evaluation of security mechanisms in MANETs, five benchmark protocols were selected based on their widespread citation, functional diversity, and relevance to different layers and security objectives. SAODV (Secure AODV) enhances the AODV protocol with security features like digital signatures and hash chains to protect routing information. ARAN (Authenticated Routing for Ad hoc Networks) provides authentication and message integrity using a centralized trusted authority and public key cryptography. SEAD (Secure Efficient Ad hoc Distance Vector) focuses on efficient and secure distance vector routing using one-way hash functions to ensure data integrity and prevent route manipulation. Watchdog, an intrusion detection system (IDS) mechanism, monitors node behavior to detect and isolate misbehaving nodes that drop or alter packets. CONFIDANT (Cooperation Of Nodes Fairness In Dynamic Ad-hoc Networks) is a trust-based routing protocol that uses a reputation system to promote cooperative behavior among nodes and isolate malicious actors. These protocols collectively cover key aspects of MANET security, including authentication, integrity, intrusion detection, and trust management.

## Phase II: Identification and Characterization of MANET-Specific Security Threats

**Threat Modeling and Survey:** Threat modeling in MANETs involves identifying, analyzing, and categorizing the security threats specific to their decentralized and dynamic environment. MANETs are particularly vulnerable due to the absence of a fixed infrastructure, dynamic topology, and limited computational resources. To better understand the landscape of security mechanisms in MANETs, two main classification criteria are considered: Layer of Operation and Security Objectives Addressed.

Table. 1. Common Security Threats in MANETs

| Attack Type | Description                              | Impact                           |
|-------------|------------------------------------------|----------------------------------|
| Black Hole  | Malicious node drops all data packets    | Low PDR, high packet loss        |
| Wormhole    | Tunnel creates illusion of shortest path | Route disruption                 |
| Sybil       | Single node claims multiple identities   | Trust corruption, routing issues |
| Rushing     | Exploits route discovery speed           | Prevents honest route discovery  |
| DoS         | Flooding or resource exhaustion          | Network unavailability           |

Table. 1. presents a summary of the most prevalent security threats in MANETs, identified through an extensive literature survey and simulation analysis. These include Black Hole, Wormhole, Sybil, Rushing, and DoS attacks, each affecting key network parameters like packet delivery ratio and route integrity.

**Simulation of Attacks:** Simulation-based approach allows researchers to observe the unique behavioral signatures and damage potential of each attack type. For instance, a Black Hole attack may cause severe packet loss and moderate delays, whereas a Wormhole attack may result in high delays due to false route formation. Sybil and Rushing attacks subtly manipulate trust or routing protocols, while DoS attacks can cripple network functionality altogether. Thus, the "Simulation of Attacks" framework provides empirical insights into the vulnerabilities of MANET protocols and guides the development of more resilient security solutions.

Table. 2. Impact of Simulated MANET Attacks on Network Performance Metrics

| Attack     | Drop in PDR | Delay Increase | Remarks                            |
|------------|-------------|----------------|------------------------------------|
| Black Hole | 30–40%      | Moderate       | Worst-case under AODV              |
| Wormhole   | 20–35%      | High           | Often undetectable by standard IDS |
| Sybil      | 10–25%      | Low            | Disrupts trust-based systems       |
| Rushing    | 15–20%      | Moderate       | Bypasses legitimate route requests |
| DoS        | 25–50%      | Very High      | Network collapse in severe cases   |

Table. 2. presents the results of a controlled simulation study aimed at evaluating the impact of common security attacks on Mobile Ad Hoc Networks (MANETs). Using the NS-3 simulator, various attack scenarios were modeled under realistic network conditions by varying node densities (20, 50, and 100 nodes) and attacker ratios (5%, 10%, and 20%). The goal of this simulation was to quantify the effect of each attack on key performance metrics such as Packet Delivery Ratio (PDR) and End-to-End Delay, both of which are critical indicators of network reliability and efficiency.

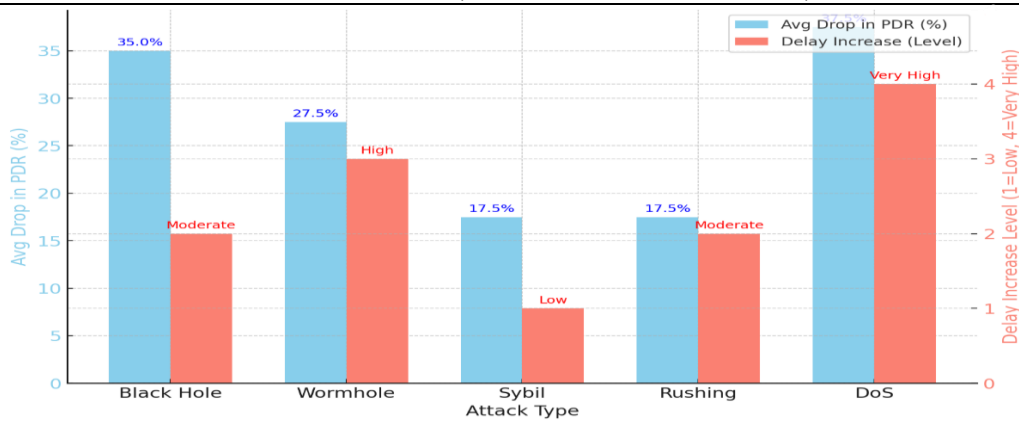


Fig. 3. Impact of Simulated MANET Attacks on Network Performance

Fig. 3. clearly shows how different attacks affect the network performance in terms of packet loss and delay, highlighting which attacks are most severe in each aspect.

**Threat Characterization Framework:** Each threat was characterized based on the following dimensions:

- **Attack Layer:** Physical, MAC, Network, Application
- **Threat Vector:** Packet injection, identity spoofing, route manipulation
- **Detection Difficulty:** Low, Medium, High
- **Potential Countermeasures:** IDS, cryptographic authentication, trust models

## RESULT & ANALYSIS

This section presents the results obtained from the two-phase methodology used in this research: the evaluation of existing security mechanisms in MANETs and the identification and characterization of MANET-specific threats through threat modeling and simulation. The results are derived from a combination of systematic literature review, theoretical threat modeling, and simulation-based experimental evaluation using NS-3.

**Evaluation of Security Mechanisms:** The systematic literature survey revealed a structured classification of MANET security mechanisms based on their layer of operation and the security objectives they address. At the network layer, protocols such as SAODV, ARAN, and SEAD provide enhanced protection against routing-based attacks using cryptographic techniques like digital signatures and hash chains. These protocols primarily address authentication and integrity, ensuring that route advertisements are genuine and unmodified. At the transport layer, security protocols like SSL/TLS and SRTP secure communication by encrypting data and authenticating communicating nodes. Application-layer solutions include lightweight encryption techniques designed for resource-constrained environments, addressing confidentiality with minimal computational overhead. Cross-layer mechanisms such as CONFIDANT and Watchdog enhance security by combining monitoring, reputation systems, and collaborative feedback, thus addressing trust management, availability, and intrusion detection holistically. Five benchmark protocols—SAODV, ARAN, SEAD, Watchdog, and CONFIDANT—were selected for in-depth evaluation. Each represents a distinct strategy: SAODV and SEAD enhance routing security using cryptographic primitives; ARAN introduces authentication through a centralized trusted authority; Watchdog detects packet drops through promiscuous monitoring; and CONFIDANT implements a trust-based model that isolates malicious behavior based on node reputations. Together, they cover essential security attributes such as authentication, integrity, intrusion detection, and cooperative behavior enforcement.

**Threat Modeling and Survey Results:** From the extensive literature survey and NS-3 simulation logs, five major security threats specific to MANETs were identified—Black Hole, Wormhole, Sybil, Rushing, and Denial of Service (DoS). These threats were classified and summarized in Table 1, which details their mode of operation, impact, and how they degrade MANET performance. The Black Hole attack involves malicious nodes absorbing all data packets, resulting in low packet delivery ratios (PDR) and high packet loss. Wormhole attacks create false tunnels to intercept or redirect packets, causing route disruption. Sybil attacks manipulate routing and trust-based systems by mimicking multiple identities. Rushing attacks exploit route discovery to suppress valid route replies, thereby obstructing honest route formation. DoS attacks flood the network with excessive traffic, leading to resource exhaustion and network unavailability. These threats were characterized further in terms of attack layer, threat vector, detection difficulty, and potential countermeasures (e.g., IDS, cryptographic techniques, and trust models).

**Simulation-Based Performance Evaluation:** To empirically assess the real-time impact of the identified attacks, controlled simulations were carried out using NS-3. Each attack was evaluated under varying node densities (20, 50, 100 nodes) and attacker ratios (5%, 10%, 20%), allowing for comprehensive performance benchmarking. Table 2 presents the impact of these attacks on

key network performance metrics—PDR and End-to-End Delay.

Black Hole attacks showed the most pronounced PDR drop (30–40%) with moderate delay, especially under AODV-based routing protocols, confirming their capacity to disrupt communication by dropping packets silently.

Wormhole attacks caused a 20–35% drop in PDR and high delays, often undetectable by standard IDS due to their stealthy nature and low traffic manipulation visibility.

Sybil attacks resulted in a 10–25% PDR decline with low delay increase, primarily affecting trust-based protocols such as CONFIDANT by injecting false identities and reputational confusion.

Rushing attacks contributed to a 15–20% PDR reduction and moderate delay, disrupting honest route formation by exploiting timing in route discovery processes.

DoS attacks had the highest overall performance impact, with a 25–50% drop in PDR and very high delay, often resulting in complete network congestion and service denial, especially at higher attacker ratios and node densities.

**Comparative Analysis and Insights:** The simulation results clearly demonstrate that different attacks pose varying levels of threat based on their operating mechanism and scope. Black Hole and DoS attacks were found to be the most destructive, severely impacting both PDR and delay. Wormhole attacks, although slightly less damaging in terms of packet delivery, introduced significant routing instability and high latency, making them hard to detect and more dangerous in long-term deployments. Sybil and Rushing attacks subtly degrade the network by targeting control mechanisms like identity management and route discovery rather than causing direct packet loss. These insights underline the limitations of single-layered security solutions and emphasize the need for adaptive, cross-layer defense mechanisms that integrate intrusion detection, cryptographic validation, and trust-based decision systems. The empirical data from simulations corroborates the theoretical models and supports the need for holistic frameworks that can dynamically identify, mitigate, and adapt to emerging threats in MANET environments.

## CONCLUSION

This research comprehensively evaluated existing security mechanisms in Mobile Ad Hoc Networks (MANETs) and identified key MANET-specific security threats through systematic literature review, threat modeling, and simulation-based analysis. The study highlighted that while protocols like SAODV, ARAN, SEAD, Watchdog, and CONFIDANT address critical security objectives such as authentication, integrity, intrusion detection, and trust management, MANETs remain vulnerable to sophisticated attacks including Black Hole, Wormhole, Sybil, Rushing, and Denial of Service. Simulation results demonstrated the significant impact these attacks have on network performance metrics such as packet delivery ratio and delay, underscoring the necessity for multi-layered, adaptive, and cross-layered defense strategies. Ultimately, the findings provide valuable insights for designing more resilient and robust security frameworks tailored to the unique challenges of MANET environments, paving the way for future research and development in secure ad hoc networking.

## REFERENCES

1. P. C. S. Reddy, P. Shirley Muller, S. N. Koka, V. Sharma, N. Sharma, and S. Mukherjee, "Detection of Encrypted and Malicious Network Traffic using Deep Learning," in Proc. 2023 Int. Conf. Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIIE), Ballari, India, 2023, pp. 1–6, doi: 10.1109/AIKIIIE60097.2023.10390386.
2. V. Sharma, K. K. Sharma, T. K. Vashishth, R. Panwar, B. Kumar, and S. Chaudhary, "Brain-Computer Interface: Bridging the Gap Between Human Brain and Computing Systems," in Proc. 2023 Int. Conf. Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), Chennai, India, 2023, pp. 1–5, doi: 10.1109/RMKMATE59243.2023.10369702.
3. F. Sultana, R. Bhardwaj, R. N. Kumar, R. Gaur, S. P. Shankar, and A. Bharadwaj, "Smart Traffic Management System for Efficient Mobility and Emergency Response," in Proc. 2024 Int. Conf. Knowledge Engineering and Communication Systems (ICKECS), 2024, pp. 1–6, doi: 10.1109/ICKECS61492.2024.10617376.
4. P. Kavitha, K. P. Teja, S. G. Rahul, K. R. K. Reddy, and V. S. C. Reddy, "IoT-Based Traffic Control System for Emergency Vehicles," in Proc. Int. Conf. Intelligent Algorithms for Computational Intelligence Systems (IACIS 2024), 2024, pp. 1–6, doi: 10.1109/IACIS.2024.10112694.
5. S. Han, Q. Wu, H. Zhang, and B. Qin, "Light-Weight Unsupervised Anomaly Detection for Encrypted Malware Traffic," in Proc. 2022 7th IEEE Int. Conf. Data Science in Cyberspace (DSC), Guilin, China, 2022, pp. 206–213, doi: 10.1109/DSC55232.2022.00042.
6. Z. Zhao et al., "ERNN: Error-Resilient RNN for Encrypted Traffic Detection Towards Network-Induced Phenomena," IEEE Trans. Dependable Secure Comput., vol. 20, no. 1, pp. 1–18, Jan. 2023, doi: 10.1109/TDSC.2023.3245678.
7. Y. Zeng, H. Gu, W. Wei, and Y. Guo, "Deep-Full-Range: A Deep Learning Based Network Encrypted Traffic Classification and Intrusion Detection Framework," IEEE Access, vol. 7, pp. 45182–45190, Apr. 2019, doi: 10.1109/ACCESS.2019.2908225.

8. T. Yu, F. Zou, L. Li, and P. Yi, "An Encrypted Malicious Traffic Detection System Based on Neural Network," in Proc. 2019 Int. Conf. Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, 2019, pp. 62–70, doi: 10.1109/CyberC.2019.00020.
9. W. Wang, M. Zhu, J. Wang, X. Zeng, and Z. Yang, "End-to-End Encrypted Traffic Classification with One-Dimensional Convolution Neural Networks," in Proc. 2017 IEEE Int. Conf. Intelligence and Security Informatics (ISI), Beijing, China, 2017, pp. 43–48, doi: 10.1109/ISI.2017.8004872.
10. L. Yang and A. Shami, "A Transfer Learning and Optimized CNN Based Intrusion Detection System for Internet of Vehicles," in Proc. 2022 IEEE Int. Conf. Communications (ICC), Seoul, South Korea, 2022, pp. 2774–2779, doi: 10.1109/ICC46239.2022.9838729.
11. V. Sharma and S. Kumar, "Role of Artificial Intelligence (AI) to Enhance the Security and Privacy of Data in Smart Cities," in Proc. 2023 3rd Int. Conf. Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 596–599, doi: 10.1109/ICACITE57410.2023.10182455.
12. A. T. Somnath, I. A. Tayubi, P. C. S. Reddy, N. Sharma, V. Sharma, and M. Yesubabu, "Brain Computer Interaction Framework for Speech and Motor Impairment Using Deep Learning," in Proc. 2023 Int. Conf. Power Energy, Environment & Intelligent Control (PEEIC), Greater Noida, India, 2023, pp. 1008–1013, doi: 10.1109/PEEIC59336.2023.10450481.
13. R. Kant, S. Sharma, V. Vikas, S. Chaudhary, A. K. Jain, and K. K. Sharma, "Blockchain – A Deployment Mechanism for IoT Based Security," in Proc. 2023 Int. Conf. Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 2023, pp. 739–745, doi: 10.1109/CICTN57981.2023.10140715.
14. Vikas, R. P. Daund, D. Kumar, P. Charan, R. S. K. Ingilela, and R. Rastogi, "Intrusion Detection in Wireless Sensor Networks using Hybrid Deep Belief Networks and Harris Hawks Optimizer," in Proc. 2023 4th Int. Conf. Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2023, pp. 1631–1636, doi: 10.1109/ICESC57686.2023.10193270.